EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	EXDIR		X (Cover Only)		
4	D/ICS		X (Cover for C/, SECOM)		
5	DDI				
6	DDA	X (For D/Comm)			
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/Pers				
14	D/OLL				
15	D/PAO				
16	SA/IA				
17	AO/DCI				
18	C/IPD/OIS				
19	NIO				
20					
21					
22					
	SUSPENSE				

Date

Remarks

STAT

Executive Secretary

17 Jan 85

Date

3637 (10-81)

NTISSC
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

OFFICE OF THE EXECUTIVE SECRETARY

NTISSC 1-3/57-85
4 January 1985

MEMORANDUM FOR THE MEMBERS OF THE NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

SUBJECT: Draft National Telecommunications and Information Systems Security Instruction (NTISSI), "Controlled COMSEC Items" - ACTION MEMORANDUM

1. Enclosed is the draft NTISSI, subject as above, dated 28 December 1984. This instruction establishes a new category of secure communications equipments and cryptographic components which are unclassified but controlled and prescribes control requirements.

2. Request you review the instruction and provide comments to the undersigned by 31 January 1985. After consideration of your comments, the NTISSI will be submitted to the National Manager for promulgation. The point of contact on this matter is

STAT [redacted] ((301) 688-6010, AUTOVON 235-6010,
AUTOSEVOCOM 2100).

STAT [redacted]

Encl:
a/s

FOR OFFICIAL USE ONLY

28 DEC 1984

DRAFT

NTISSI No.----
Date:

FOREWORD

1. National Telecommunications and Information Systems Security Instruction (NTISSI) No. ----, "Controlled COMSEC Items," establishes a new category of secure communications equipments and cryptographic components which are unclassified but controlled, and redefines the designator "Controlled COMSEC Item" (CCI). This Instruction also prescribes the requirements for controlling the new category of equipments and components.

2. This Instruction is effective immediately. Additional copies may be obtained from:

Executive Secretariat
National Telecommunications and Information
Systems Security Committee
National Security Agency
Fort George G. Meade, Maryland 20755-6000

3. This Instruction is not releasable to foreign nationals without the specific approval of the Director, National Security Agency (DIRNSA).

4. Extracts of information from this Instruction may be made as necessary. Such extracts shall be marked "FOR OFFICIAL USE ONLY," and shall not be made available to the general public without the specific approval of DIRNSA.

5. Federal departments and agencies shall implement this Instruction within 120 days of the effective date. One copy of each department or agency implementing directive shall be forwarded to DIRNSA, ATTN: S, for review and approval.

LINCOLN D. FAURER
National Manager
National Telecommunications
and
Information Systems Security

DRAFT

FOR OFFICIAL USE ONLY

DRAFT NTISS No. ----

CONTROLLED COMSEC ITEMS

1. REFERENCES. Reference is made within this Instruction to the following publications. The requirements of the references apply to this Instruction to the extent specified herein.

a. NACSI No. 4005, "Safeguarding and Control of Communications Security Material," dated 12 October 1979.

b. NACSI No. 4006, "Reporting COMSEC Insecurities," dated 20 October 1983.

c. NACSI No. 4010, "Routine Destruction and Emergency Protection of COMSEC Material," dated 23 February 1982.

d. NCSC-2, "National Policy on Release of Communications Security Information to U.S. Contractors and Other U.S. Nongovernmental Sources," dated 7 July 1983.

e. NCSC-6, "National Policy Governing the Disclosure or Release of Communications Security Information to Foreign Governments and International Organizations," dated 16 January 1981.

f. NACAM-83/1, "Advisory Memorandum on Protection of Communications Security Information Released to Foreign Governments and International Organizations," dated 10 June 1983.

g. NCSC-9, "National Communications Security (COMSEC) Glossary," dated 1 September 1982.

NOTE: Several General COMSEC Doctrine (4000-series) NACSIs will require revision to accommodate the new Controlled COMSEC Item (CCI) concept introduced by this Instruction. In the interim, where the requirements of a 4000-series NACSI conflict with those of this Instruction, the requirements of this Instruction shall take precedence.

2. PURPOSE AND BACKGROUND.

a. The new CCI category applies to specified, unclassified, secure communications equipments and cryptographic components. The intent is to promote the broad

expansion of secure communications for the protection of national security (classified), as well as national security-related (unclassified) and other information which should be protected in the national interest. It is an element of the National Security Agency (NSA) initiative to expand the use of secure communications equipments.

b. Secure communications equipments and cryptographic components which are designated "Controlled COMSEC Item," or "CCI," employ a classified cryptographic logic, and it is only the hardware or firmware embodiment of that logic which is unclassified. The associated cryptographic engineering drawings, logic descriptions, theory of operation, computer program listings, and related cryptographic information remain classified.

c. Procedures for controlling CCI secure communications equipment and cryptographic components are required to guard against preventable losses to an actual or potential enemy. However, in keeping with the spirit of expanded use of secure communications equipments, minor lapses in carrying out control procedures shall be dealt with locally as a matter of administrative discretion. More serious infractions involving, for example, sabotage, loss through gross negligence, theft, or espionage are punishable under various sections of the United States Code or the Uniform Code of Military Justice.

3. APPLICABILITY. This Instruction applies to all departments and agencies of the U.S. Government, and their contractors, who handle, distribute, account for, store, or use CCI secure communications equipments and cryptographic components.

4. DEFINITIONS. The definitions contained in NCSC-9 apply to this Instruction, with the exception that the NCSC-9 definition of "Controlled COMSEC Item (CCI)" is superseded by the definition given below. Also given below are additional, special definitions which apply to this Instruction.

a. Controlled COMSEC Item (CCI). A secure communications equipment or cryptographic component which is unclassified but controlled. Equipments and components so designated shall bear the marking "Controlled COMSEC Item" or "CCI."

b. Secure Communications Equipment. Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and by reconverting such information to its original form for authorized recipients. Secure

communications equipments may be stand-alone crypto-equipments, as well as communications equipments with integrated or embedded cryptography.

c. Cryptographic Component. The hardware or firmware embodiment of the cryptographic logic in a secure communications equipment. A cryptographic component may be a modular assembly, a printed circuit board, a microcircuit, or a combination of these items.

5. RESPONSIBILITIES.

a. The Director, National Security Agency (DIRNSA), is responsible for:

(1) Determining which existing and future equipments and components are to be designated as CCI. (User departments and agencies may recommend equipments and components for designation as CCI. Such recommendations should include supporting documentation.)

(2) Establishing requirements for controlling CCI equipments and components.

(3) Ensuring that equipments and components designated as CCI are marked with the designator "CONTROLLED COMSEC ITEM" or "CCI."

(4) Issuing new or revised COMSEC system doctrine for equipment designated CCI.

b. The heads of departments and agencies are responsible for implementing approved procedures for controlling CCI secure communications equipments and cryptographic components in accordance with this Instruction or other national issuances, as appropriate.

6. CONTROL REQUIREMENTS. The following subparagraphs set forth the minimum requirements for controlling unkeyed CCI equipments and components. Where such equipments and components contain classified key, they shall be protected in accordance with the requirements of NACSI No. 4005. Also, depending upon the application, other more stringent requirements may be prescribed.

a. Access. A security clearance is not required for access to CCI equipments and components. However, access shall be restricted to individuals whose duties require such access. The provision of CCI equipment or components to U.S. individuals who are not part of the U.S. Government is covered by NCSC-2; and to foreign governments and international organizations by NCSC-6 and NACAM-83/1.

b. Storage. CCI equipments and components shall be stored in a manner that affords protection at least equal to that which is normally provided to other high-value property.

c. Transportation. CCI equipments and components shall be transported by a means which ensures that access, storage, and accounting integrity is maintained.

d. Accounting. CCI secure communications equipments and cryptographic components shall be accounted for at a central point within each department or agency, as follows:

(1) CCI equipments shall be accounted for by serial number. Separate accountability is not required for CCI components installed in these equipments. Spare or other uninstalled CCI components shall be accounted for by quantity.

(2) The accounting system must provide the following:

(a) The identification of CCI equipments and components which are lost.

(b) Individual accountability in order to support prosecution in cases which involve espionage.

(3) CCI accounting data at the central point shall be available to NSA via on-line or other readily accessible means.

e. Inventories. Within each major organization that accounts directly to the central point, CCI equipments and uninstalled CCI components shall be inventoried at least annually. Inability to reconcile a major organization's holdings of these equipments and components with the record of accountability at the central point shall be reported as a COMSEC insecurity in accordance with NACSI No. 4006.

f. Reporting Insecurities. The insecurities reporting requirements of NACSI No. 4006 apply to CCI equipments and components.

g. Routine and Emergency Destruction. The routine and emergency destruction standards and procedures of NACSI No. 4010 apply to CCI equipments and components.